

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

**Студенттер мен жас ғалымдардың
«GYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«GYLYM JÁNE BILIM - 2024»**

**PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«GYLYM JÁNE BILIM - 2024»**

**2024
Астана**

УДК 001

ББК 72

G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докторанттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001

ББК 72

G99

ISBN 978-601-7697-07-5

**©Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2024**

АЛГОРИТМ НАСТРОЙКИ И ПРИМЕНЕНИЯ WSL В ХОДЕ КРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА НОСИТЕЛЕЙ ИНФОРМАЦИИ

Бөлек Жандәулет Сырымұлы

zh.bolek@gmail.com

студент III курса образовательной программы 6B06306 «Системы информационной безопасности», Евразийский национальный университет им. Л. Н. Гумилева
Научный руководитель Токкулиева Айжан Конурбаевна

Защита данных становится все более критической задачей, особенно когда речь идет о флеш-накопителях [1]. В таких ситуациях методика использования Kali Linux через Windows Subsystem for Linux (WSL) выделяется как надежный и безопасный способ анализа данных на флеш-носителях.

Установка Kali Linux через WSL предоставляет ряд преимуществ. Во-первых, она позволяет создать изолированную среду для анализа данных, что минимизирует риск заражения основной операционной системы в случае обнаружения вредоносных элементов на флеш-накопителе. Кроме того, процесс установки прост и доступен даже для непрофессионалов, что делает использование Kali Linux через WSL легким и удобным.

Однако основное преимущество этой методики заключается в возможности использования инструментов The Sleuth Kit, входящих в состав Kali Linux [2,3]. The Sleuth Kit предоставляет широкий спектр утилит для анализа файловых систем и создания образов носителей данных. Эти инструменты позволяют проводить глубокий анализ флеш-накопителей, включая поиск удаленных файлов и проверку наличия вредоносных программ.

Стоит также отметить, что WSL представляет собой альтернативу виртуальным машинам, таким как VirtualBox. Однако в некоторых случаях, особенно в криминалистике, использование WSL для анализа данных на флеш-накопителях находится вне конкуренции благодаря удобству интеграции с операционной системой Windows. Это делает процесс анализа более удобным и эффективным для специалистов, работающих с данными в сфере криминалистики и цифровой безопасности.

Ниже представлен алгоритм настройки среды для дальнейшего криминалистического анализа образов носителей в Windows с помощью инструментария Linux.

Для установки Kali Linux на Windows через WSL необходимо загрузить и установить ее через Microsoft Store [4,5]. После установки необходимо прописать следующие команды в командной строке (см.рис.1):

\$ sudo su	<i>переход в режим администратора</i>
# apt-get update	<i>обновление пакетов</i>
# apt-get dist-upgrade	<i>обновление системы</i>
# sudo apt install kali- win-kex	<i>инструменты для запуска графических приложений Windows на Kali Linux</i>
#kex --win -s	<i>запуск графической среды</i>

Установка Sleuth Kit на Kali Linux. The Sleuth Kit - это набор бесплатных инструментов для анализа данных на компьютере. Он помогает экспертам по безопасности и следователям извлечь информацию из жестких дисков, флэш-накопителей и других устройств хранения данных. С помощью команд fls, icat, fsstat, mactime, blkls и blkstat можно выполнять детальный анализ файловой системы на предмет извлечения цифровых улик [1,3].

Подключение флэш-накопителя к WSL. Для анализа флэш-накопителей нужно установить ряд программ:

1. usbipd-win - программное обеспечение Windows для совместного использования локально подключенных USB-устройств с другими машинами, включая гостей Hyper-V и WSL 2 [4].

2. WSL USB Manager - программа с графическим интерфейсом позволяющая управлять устройствами (рис.2) [5].

```

(zhandaulet@ZHD) ~$ sudo su
[sudo] password for zhandaulet:
(zhandaulet@ZHD) ~$ # apt-get update
Get:1 http://mirror.cspacehostings.com/kali kali-rolling InRelease [41.5 kB]
Get:2 http://mirror.cspacehostings.com/kali kali-rolling/main amd64 Packages [19.5 MB]
16% [2 Packages 1,185 kB/19.5 MB 6%]

(zhandaulet@ZHD) ~$ # apt-get dist-upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
(zhandaulet@ZHD) ~$ # sudo apt install kali-win-kex
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  7zip accountsservice acl admaita-icon-theme alsa-topology-conf
  alsa-ucm-conf aspell aspell-en at-spi2-common at-spi2-core atril
  atril-common avahi-daemon blueman bluez bluez-obexd bsdxtractils
  bubblewrap busybox bzip2 catfish colord colord-data cpp cpp-13
(zhandaulet@ZHD) ~$ # kex --win -s
Starting Win-KeX server (Win)
Password:
Password must be at least 6 characters - try again
Password:
Verify:
Passwords don't match - try again
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
Win-KeX server (Win) is running

Win-KeX server sessions:
X DISPLAY #      RFB PORT #      RFB UNIX PATH      PROCESS ID #      SERVER
2             5902             /dev/fd/3           22119             Xtigervnc

You can use the Win-KeX client (Win) to connect to any of these displays

Starting Win-KeX client (Win)
  
```

Рисунок 1. Начальная настройка WSL.

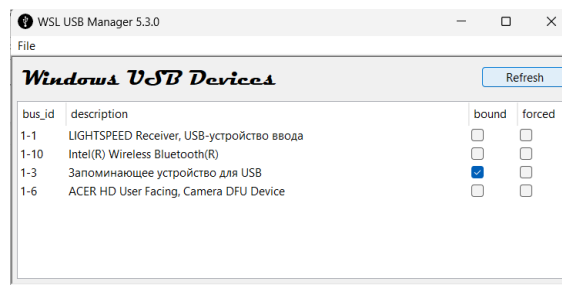


Рисунок 2. WSL USB Manager для подключения флэш накопителей к WSL.

Процесс создания образа флэш-накопителя с использованием Sleuth Kit. Для создания криминалистического образа носителя были использованы команды lsblk, dd, md5sum. Подробный пример использования указанных команд продемонстрирован на рисунке 3.

```

(zhandaulet@ZHD) ~$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda         8:0    0 388.5M  1 disk
sdb         8:16   0    2G    0 disk [SWAP]
sdc         8:32   0    1T    0 disk /mnt/wslg/distro
sdd         8:48   0    1T    0 disk

(zhandaulet@ZHD) ~$ # sudo dd if=/dev/sdb of=backup.dd status=progress
7798505984 bytes (7.8 GB, 7.3 GiB) copied, 450 s, 17.3 MB/s
15261696+0 records in
15261696+0 records out
7813988352 bytes (7.8 GB, 7.3 GiB) copied, 451.061 s, 17.3 MB/s

(zhandaulet@ZHD) ~$ # md5sum backup.dd
404c77fa96a0512a0542d24bba0ced24  backup.dd
  
```

Рисунок 3. Создание образа диска.

Анализ образа носителя и просмотр удаленных файлов. Следующие группа команд используется для детального анализа файловой системы полученного на предыдущем этапе

криминалистического образа. А именно просмотр статистики файловой системы, структура разделов и списка удаленных файлов `img_stat`, `fsstat`, `fls`, `icat`, `istat`, (рис. 4–8) [1,2,3].

```

(zhandaulet@ZHD) ~/Desktop/usb
└─$ img_stat example.dd
IMAGE FILE INFORMATION
-----
Image Type: raw
Size in bytes: 7812939776
Sector size: 512
  
```

Команда `img_stat` отображает размер файла, размер сектора и т.

Рисунок 4. Вывод статистики образа `example.dd` с помощью команды `img_stat`

```

(zhandaulet@ZHD) ~/Desktop/usb
└─$ fsstat example.dd
FILE SYSTEM INFORMATION
-----
File System Type: FAT32
SEM Name: MSDOS5.0
Volume ID: 0-b00041f2
Volume Label (Boot Sector): NO NAME
Volume Label (Root Directory): ESD-USB
File System Type Label: FAT32
Next Free Sector (FS Info): 32864
Free Sector Count (FS Info): 15226784
Sectors before file system: 2848

File System Layout (in sectors)
Total Range: 0 - 15259647
* Reserved: 0 - 3025
** Boot Sector: 0
** FS Info Sector: 1
** Backup Boot Sector: 6
* FAT 0: 3026 - 17896
* FAT 1: 17897 - 32767
* Data Area: 32768 - 15259647
** Cluster Area: 32768 - 15259647
** Root Directory: 32768 - 32775

METADATA INFORMATION
-----
Range: 2 - 243630086
Root Directory: 2

CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 2 - 1983361

FAT CONTENTS (in sectors)
-----
32768-32775 (8) -> EOF
32776-32783 (8) -> EOF
32784-32791 (8) -> EOF
32792-32799 (8) -> EOF
32800-32831 (32) -> EOF
32832-32839 (8) -> EOF
32840-32863 (24) -> EOF
  
```

`fsstat` – выводит информацию о файловой системе, содержащейся в образе диска `example.dd`. В данном случае файловая система определена как FAT32. Команда предоставляет информацию о различных аспектах файловой системы, таких как метаданные, содержимое, размер сектора и размер кластера, а также

Рисунок 5. Применение команды `fsstat` для вывода информации о файловой системе.

```

(zhandaulet@ZHD) ~/Desktop/usb
└─$ fls example.dd
r/r 3: ESD-USB (Volume Label Entry)
d/d 6: System Volume Information
/r/r * 9: Боек Жандаулет-Отчет.docx
/r/r 11: ex1.docx
/r/r 12: ex2.txt
/r/r 14: ex3.xlsx
v/v 243630083: $MBR
v/v 243630084: $FAT1
v/v 243630085: $FAT2
v/v 243630086: $OrphanFiles

(zhandaulet@ZHD) ~/Desktop/usb
└─$ fls -d example.dd
/r/r * 9: Боек Жандаулет-Отчет.docx
  
```

`#fls -d` – выводит список удаленных файлов из образа диска `example.dd`, включая информацию о них, такую как идентификатор индекса (`inode`), тип, размер и имя файла. В данном случае выводится информация об удаленном файле "Боек Жандаулет-Отчет.docx".

Рисунок 6. Просмотр структуры образа носителя и вывод удаленных файлов.

```

(zhandaulet@ZHD) ~/Desktop/usb
└─$ icat example.dd 9 > del.docx
  
```

Рисунок 7. Восстановление удаленного файла с помощью `icat`.

```

(zhandaulet@ZHD) ~/Desktop/usb
└─$ istat example.dd 9
Directory Entry: 9
Not Allocated
File Attributes: File, Archive
Size: 325607
Name: ^^^^^~1.DOC

Directory Entry Times:
Written: 2024-03-12 16:36:40 (+05)
Accessed: 2024-03-28 00:00:00 (+05)
Created: 2024-03-28 21:58:33 (+05)

Sectors:
32800 32801 32802 32803 32804 32805 32806 32807
  
```

`#istat` - Извлекает и выводит информацию о удаленном файле с идентификатором индекса (`inode`) 9 из образа диска `example.dd`.

Рисунок 8. Анализ файловой системы исследуемого носителя.

В ходе анализа криминалистического образа носителя был восстановлен ранее удаленный файл, сделан детальный анализ файловой системы носителя и получена статистика носителя информации, необходимой в дальнейшем анализе.

Преимущества использования Kali Linux через WSL для анализа флэш-накопителей очевидны и играют ключевую роль в обеспечении безопасности данных. Во-первых, этот подход гарантирует изоляцию среды анализа, что снижает риск заражения основной операционной системы в случае обнаружения вредоносных элементов на флэш-накопителе. Во-вторых, установка и настройка Kali Linux через WSL просты и доступны даже для неопытных пользователей. Благодаря этому, широкий круг пользователей может воспользоваться мощными инструментами, такими как Sleuth Kit, который значительно упрощает создание образов флэш-накопителей и анализ удаленных данных.

Применение методики использования Kali Linux через WSL в анализе флэш-накопителей предоставляет пользователям возможность эффективно выявлять потенциальные угрозы безопасности и принимать соответствующие меры для защиты данных. Этот подход не только обеспечивает безопасность и конфиденциальность информации, но и повышает уверенность пользователей в целостности и надежности их данных.

Необходимо отметить, что создание образа флэш-накопителя с помощью утилиты dd играет ключевую роль в процессе анализа. Создание образа позволяет сохранить целостность оригинальных данных, обеспечивая более точный и надежный анализ. Таким образом, использование Kali Linux через WSL открывает новые возможности для безопасного анализа флэш-накопителей и обеспечения защиты данных в цифровой среде с использованием Windows.

Список использованных источников

1. Oh J., Lee S., Hwang H. Forensic recovery of file system metadata for digital forensic investigation //IEEE Access. – 2022. – Т. 10. – С. 111591-111606.
2. Easttom C. Digital Forensics, Investigation, and Response. – Jones & Bartlett Learning, 2021.
3. Nikkel B. Practical Linux Forensics: A Guide for Digital Investigators. – no starch Press, 2021.
4. <https://github.com/dorssel/usbipd-win/> - Windows software for sharing locally connected USB devices to other machines, including Hyper-V guests and WSL 2.
5. <https://gitlab.com/alelec/wsl-usb-gui> - WSL USB Manager to manage connecting USB devices from Windows to the WSL linux environment.

УДК 004.056.5

БОРЬБА С АКАДЕМИЧЕСКОЙ НЕЧЕСТНОСТЬЮ: ВНЕДРЕНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ В СИСТЕМЫ УПРАВЛЕНИЯ ОБУЧЕНИЕМ ДЛЯ ПРЕДОТВРАЩЕНИЯ ФАЛЬСИФИКАЦИИ ДААННЫХ

Данияров Олжас Адылканович

olzhas.danayarov@mail.ru

Евразийский национальный университет имени Л. Н. Гумилёва
Научный руководитель старший преподаватель Аймичева Г.И.

Академическая нечестность, включая практику "buddy punching" и представление чужих работ, становится все более распространенной и серьезной проблемой в образовательной среде. Это явление подрывает целостность систем оценки, а также влияет на принципы справедливости и меритократии, лежащие в основе академического сообщества. В данном контексте внедрение метода двухфакторной аутентификации (2FA), основанного на использовании QR-кодов и одноразовых паролей (OTP), в системы управления обучением (LMS) представляет собой важный шаг в борьбе с академической нечестностью. Использование 2FA для входа в систему значительно усложняет возможность злоупотребления системой и представления чужих действий как своих собственных. Этот